Hw 7

Zoe Werner

11/25/2024

Recall that in class we showed that for randomized response differential privacy based on a fair coin (that is a coin that lands heads up with probability 0.5), the estimated proportion of incriminating observations $\hat{P}$ [1] was given by $\hat{P} = 2\hat{\pi} - \frac{1}{2}$ where $\hat{\pi}$ is the proportion of people answering affirmative to the incriminating question.

I want you to generalize this result for a potentially biased coin. That is, for a differentially private mechanism that uses a coin landing heads up with probability $0 \leq \theta \leq 1$, find an estimate $\hat{P}$ for the proportion of incriminating observations. This expression should be in terms of θ and $\hat{\pi}$.

Student Answer

$\pi = \theta P + (1 - \theta)\theta$

$\hat{\pi} = \theta \hat{P} + (1 - \theta)\theta$

$\hat{P} = \frac{\hat{\pi} - (1-\theta)\theta}{\theta}$

Next, show that this expression reduces to our result from class in the special case where $\theta = \frac{1}{2}$.

Student Answer

$\pi = \theta P + (1 - \theta)\theta$

$\pi = (\frac{1}{2})P + (\frac{1}{2})(\frac{1}{2})$

$\pi = \frac{1}{2}P + \frac{1}{4}$

$\pi - \frac{1}{4} = \frac{1}{2}P$

$P = (\pi - \frac{1}{4})2$

Part of having an explainable model is being able to implement the algorithm from scratch. Let's try and do this with `KNN`. Write a function entitled `chebychev` that takes in two vectors and outputs the Chebychev or L^∞ distance between said vectors. I will test your function on two vectors below. Then, write a `nearest_neighbors` function that finds the user specified k nearest neighbors according to a user specified distance function (in this case L^∞) to a user specified data point observation.

[1] in class this was the estimated proportion of students having actually cheated

```r
#student input
#chebychev function
chebychev <- function(a,b) {
  max(abs(a-b))
}
#nearest_neighbors function
nearest_neighbors = function(x, obs, k, dist_func){
  dist = apply(x, 1, dist_func, obs)
  distances = sort(dist)[1:k]
  neighbor_list = which(dist %in% sort(dist)[1:k])
  return(list(neighbor_list, distances))
}

x<- c(3,4,5)
y<-c(7,10,1)
chebychev(x,y)
```

```
## [1] 6
```

Finally create a `knn_classifier` function that takes the nearest neighbors specified from the above functions and assigns a class label based on the mode class label within these nearest neighbors. I will then test your functions by finding the five nearest neighbors to the very last observation in the `iris` dataset according to the `chebychev` distance and classifying this function accordingly.

```r
library(class)
df <- data(iris)
#student input
knn_classifier = function(x,y){

  groups = table(x[,y])
  pred = groups[groups == max(groups)]
  return(pred)
}

#data less last observation
x = iris[1:(nrow(iris)-1),]
#observation to be classified
obs = iris[nrow(iris),]

#find nearest neighbors
ind = nearest_neighbors(x[,1:4], obs[,1:4], 5, chebychev)[[1]]
as.matrix(x[ind,1:4])
```

```
##     Sepal.Length Sepal.Width Petal.Length Petal.Width
## 71           5.9         3.2          4.8         1.8
## 84           6.0         2.7          5.1         1.6
## 102          5.8         2.7          5.1         1.9
## 127          6.2         2.8          4.8         1.8
## 128          6.1         3.0          4.9         1.8
```

```
## 139          6.0         3.0          4.8         1.8
## 143          5.8         2.7          5.1         1.9
```

```
obs[,1:4]
```

```
##     Sepal.Length Sepal.Width Petal.Length Petal.Width
## 150          5.9           3          5.1         1.8
```

```
knn_classifier(x[ind,], 'Species')
```

```
## virginica
##         5
```

```
obs[,'Species']
```

```
## [1] virginica
## Levels: setosa versicolor virginica
```

Interpret this output. Did you get the correct classification? Also, if you specified $K = 5$, why do you have 7 observations included in the output dataframe?

Student Answer I got 5/7 classifications correct. The first two values on the list, 71 and 84 were incorrectly classified as virginica while they are actually versicolor. Even though k is specificed as 5, there are 7 observations because line 63 (neighbor_list = which(dist %in% sort(dist)[1:k])) of the nearest neighbors function allows for ties in the case of duplicate values. If two datapoints are the same distance, they are both included in the k nearest neighbors list. Even though k was classified as 5, because of line 63, duplicate distances are allowed and the output was higher then the k value.

Earlier in this unit we learned about Google's DeepMind assisting in the management of acute kidney injury. Assistance in the health care sector is always welcome, particularly if it benefits the well-being of the patient. Even so, algorithmic assistance necessitates the acquisition and retention of sensitive health care data. With this in mind, who should be privy to this sensitive information? In particular, is data transfer allowed if the company managing the software is subsumed? Should the data be made available to insurance companies who could use this to better calibrate their actuarial risk but also deny care? Stake a position and defend it using principles discussed from the class.

Student Answer

According to the Consequentialism framework, sharing the healthcare data in pursuit of assisting management of acute kidney injury is morally permissible. Consequentialism states that morality is based on the outcome of an action. Since the data could be used to advance medical knowledge and technology, the outcome is highly beneficial. However, if it is going to be released to an exterior company, the customers should be alerted to this and have the opportunity to provide informed consent. If consent is obtained through terms and conditions, most users will not take the time to read it and will unknowingly agree to data sharing, which is not informed consent. Tacit consent is another moral alternative. Currently, Google DeepMind does not charge a subscription or one-time fee for users. This is possible through software sales,

but selling data is another form of profit that prevents users from paying for the service. Even if users consent to the terms and conditions without full understanding, they are benefiting from the service and therefore, Google obtained tacit consent.

Sharing the sensitive healthcare data becomes immoral when insurance companies become involved. According to Utilitarianism, an act is morally permissible when the pleasures are more abundant then pain. If insurance agencies gained access to healthcare data, they could use it to deny coverage to people who are chronically ill, have biological indicators for chronic disease, and others who desperately need healthcare. The insurance companies would benefit by excluding cost-heavy customers, but lack of healthcare would cause great pain for many people.

I have described our responsibility to proper interpretation as an *obligation* or *duty*. How might a Kantian Deontologist defend such a claim?

Student Answer

Immanuel Kants categorical imperative formulation one states that an act is moral if it can be universalized in society without logical contradiction. If we do not treat proper interpretation as an obligation or duty, it could not be categorized as moral becuase this practice could not be universalized in society. If proper interpretation was completely erased from society, all conclusions would be incorrect and therefore, worthless. If any sort of meaningful statistical conclusion is seeked, proper interpretation is necessary. The first formulation requires proper interpretation to be considered an obligation because if it valued as less, it would violate the universal maxim. If it was universalized, it would cause contradiction in society.

The second formulation requires all moral agents to be treated as ends, rather then solely means to an end. In other words, an act is not moral if someone instrumentalizes people in the process. Depending on the dataset, improper interpretation may violate this formulation. If the dataset is based on information from people (aka moral agents), using it to support improper conclusions is using them as a means to an end. The data cannot be used to better the people involved. If the people agreed to involvement to help a cause or seek a truthful answer or solution, they are being cheated out of an honest result. Therefore, they are being treated as a means to an end because they are not receiving a fair interpretation and are deprived their end of the tacit consent. Overall, both of Kants categorical imperatives support the classification of proper interpretation as an obligation or duty. If data is properly interpreted, the people involved are not treated as a means to an end (unless unknown factors are at play) and the universal action would be acceptable in society.